



Enterprise Income Verification (EIV) System

Rules of Behavior and User Agreement

HUD Office or Field

Office Name: _____

(To be completed by HUD employees/contractors)

HUD Field Office Code: _____

(e.g. 1HBOS)

PHA Name: _____

(To be completed by PHA employees/contractors)

PHA Code: _____

(e.g. MD999)

A. Rules of Behavior

1. Introduction

The U.S. Department of Housing and Urban Development (HUD), Public and Indian Housing Real Estate Assessment Center (PIH-REAC) is actively involved in implementing and maintaining Office Departmental policies and procedures to keep PIH-REAC Systems secure from unauthorized access and inappropriate use. In compliance with various security-related Federal laws and regulations, PIH-REAC created these rules of behavior for the Enterprise Income Verification (EIV) system. This document was created to ensure that EIV system users comply with HUD and PIH-REAC security policies. In addition, this document ensures that system accounts remain secure and are used in the appropriate manner.

PIH-REAC may grant limited system access to users (e.g. HUD employees, contractors, clients/customers, and program participants) who have a need to utilize the PIH-REAC information resources. EIV resources are for official use only. As a condition of receiving access, you are required to understand and abide by the HUD and PIH-REAC's EIV system security policies and procedures. The purpose of these policies and procedures is to safeguard the PIH-REAC's valuable information resources.

All EIV users must adhere to the Rules of Behavior outlined in this document. The rules clearly delineate responsibilities of, and expectations for, all individuals with access to the EIV system. Non-compliance with these rules will be disciplined through sanctions commensurate with the level of infraction. This may include removal of system access for a specific period of time or termination depending on the severity of the violation. See Section B for potential civil and criminal penalties.

2. Responsibilities

The System Owner is responsible for ensuring that an adequate level of protection is afforded to the EIV system through an appropriate implementation of technical, operational, and managerial security controls.

EIV system users are responsible for the protection of passwords, information, equipment, systems, networks, and communication pathways to which they have access. All HUD computer resources including hardware, software, programs, files, paper reports, and data are the sole property of HUD.

3. Other Policies and Procedures

The Rules of Behavior do not replace existing HUD or PIH-REAC policy, rather they are intended to enhance and further define the specific rules each user must follow while accessing the EIV system. The rules are consistent with the policy and procedures described in the following security documents:

HUD Security Program Policy The policy, HUD Handbook 2400.25, Rev. 1 dated May 2005, prescribes responsibilities, practices, and conditions that directly or indirectly promote security in the development, operation, maintenance, and support of all HUD IT resources.

4. Application Rules

The Web Access Security System (WASS) user identification (userID) and password issued to you are to be used solely in connection with the performance of your responsibilities in support of HUD's mission and may not be used for personal or private gain. You agree to be responsible for the confidentiality of the assigned information and accountable for all activity with your userID. Furthermore, you agree that you will not provide this confidential userID/password to another user during employment and upon leaving the employment of the Department. Additional rules of the EIV system are as follows:

System Access (on-site only) – Users are required to use only approved HUD software, software settings, and comply with vendor software license agreements. Users are allowed to access the system only using the mechanisms specified by PIH-REAC.

Unofficial use of government information – Users must be aware that personal use of information resources is prohibited. EIV data is personal information covered by the Privacy Act and penalties apply to the misuse of that data.

Information protection – Users must avoid leaving system output records or reports unattended or unsecured. Users should lock the computer or log-out of the system when leaving work areas unattended. Users shall not violate Public Law 93-579, Privacy Act of 1974, which requires confidentiality of personal data contained in government and contractor data files. Users should back up their data, test the data backups, and securely store the data in accordance with PIH-REAC policy.

Use of passwords – User passwords and userIDs are for your individual use only and are confidential HUD information. Users are required to change passwords every 21 days. Users are encouraged to avoid creating passwords that can be easily associated with.

System privileges – Users are given access to the system based on a need to perform specific work. Users shall only access the information for which they are authorized.

Individual accountability – Users shall be held accountable for their actions while accessing the system. Be aware that all computer resources are monitored and audited.

Incident Response – Users should contact their supervisor and the PIH-REAC Security Officer immediately regarding any suspected violation or breach of system security.

B. User Agreement

I have read the above policy regarding system security awareness and practices when accessing PIH-REAC's information technology resources. I understand the policies and procedures as set forth above, and I agree to comply with these requirements as a condition of being granted limited access to the Enterprise Income Verification System and data.

As an authorized user of the Enterprise Income Verification System, I understand the information obtained may only be used for official HUD/PHA business. I understand that only authorized HUD or PHA employees may access, disclose, inspect and use upfront income verification (UIV) data.

I also understand that willful unauthorized inspection of UIV data can result in civil and criminal penalties. The penalties are as follows:

- **Unauthorized disclosure** can result in a felony conviction and a fine of up to \$5,000 and/or imprisonment up to five (5) years, as well as civil penalties.
- **Unauthorized inspection** of UIV data can result in a misdemeanor penalty of up to \$1,000 and/or one (1)-year imprisonment, as well as civil damages.

I understand that my user ID and password are to be used only by me. Under no circumstances will I reveal or allow use of my password by another person. Nor will I use another person's password and user ID.

I understand and agree to follow all HUD/PHA standards, policies and procedures.

EIV System User's Name
(Signature)

EIV System User's Name
(Print)

Date

Copy – File